Lexicographic Configurations

Christoph Hering[*] Andreas Krebs[†] Thomas Edgar[‡]

November 9, 2012

Abstract

We describe a new way to construct finite geometric objects. For every k we obtain a symmetric configuration $\mathcal{E}(k-1)$ with k points on a line. In particular, we have a constructive existence proof for such configurations. The method is very simple and purely geometric. It also produces interesting periodic matrices.

Keywords : Configurations, projective planes.
MSC 2010 classification : 51E15, 05B15

1 Introduction

In this paper we describe a new geometric way to construct finite projective planes and finite symmetric configurations. It concerns a first choice construction that is very elementary. Notably, it produces an interesting finite incidence geometry $\mathcal{E}(n)$ for every rational integer n. $\mathcal{E}(n)$ is a symmetric configuration of order n, that is, an incidence geometry $\mathcal{E}(n) = (\mathcal{P}, \mathcal{B})$ consisting of a non-empty set $\mathcal{P}$ of elements, which we call *points*, and a set $\mathcal{B}$ of subsets of $\mathcal{P}$, which we call *blocks*, such that

(i) if b and b' are blocks, then $|b \cap b'| \leq 1$,

(ii) $|b| = n + 1$ for all $b \in \mathcal{B}$, and

(iii) every point $p \in \mathcal{P}$ is contained in exactly $n + 1$ blocks in $\mathcal{B}$.

Here $|\mathcal{P}| \geq n^2 + n + 1$. If $|\mathcal{P}| = n^2 + n + 1$ and $n \geq 2$, then $(\mathcal{P}, \mathcal{B})$ actually is a projective plane.

[*]Institute of Mathematics of the University of Tübingen, Auf der Morgenstelle 10, 72076 Tübingen, Germany,
email: hering@uni-tuebingen.de
[†]Wilhelm-Schickard-Institute, University of Tübingen, Sand 13, 72076 Tübingen, Germany,
email: krebs@informatik.uni-tuebingen.de
[‡]United States Army, Army Europe Libraries, Stuttgart Library
email: thomas.b.edgar@us.army.mil

In infinitely many cases, our construction leads to the symmetric configuration $\mathcal{E}(n)$ very rapidly. We obtain, for example, a completely geometric construction of the projective planes PG(2,16) and PG(2,256) (and thereby of GF(16) and GF(256)) without requiring any algebraic foundations. In the general case, however, the calculations appear to be very long, as we shall see in Section 5.

We can, however, easily prove that for every integer $k \geq 1$ there exists a symmetric configuration with k points on each line (allowing a sufficiently large number of points).

In light of the fact that there do not exist projective planes of the orders 6 or 10 (see Section 5), we are lead to the problem of determining $\mathcal{E}(6)$ and $\mathcal{E}(10)$. It might be interesting to know what these symmetric configurations are. Although it is possible and indeed simple to calculate $\mathcal{E}(5)$, already for $\mathcal{E}(6)$ we needed 3 months of computer time on a usual desktop PC, and, until now, we were not able to determine $\mathcal{E}(10)$ (see Section 5).

With some further effort, the method can be generalized to general (possibly not symmetric) configurations. Then we obtain a much wider variety of geometries. In particular, we find many more cases which can be finished after a rather short computation. For example, we find point-line geometries of higher dimensional projective spaces, Steiner triple systems and the like (see [8]).

Additionally, the construction provides an example of an extremely frugal first choice construction which succeeds efficiently in rather complex situations.

The starting point and many of the results of this paper originate from the Diploma Thesis of one of the authors, Thomas Edgar. We are very grateful to Hans-Joerg Schaeffer for many useful remarks and computational support.

2 The notation

$\mathbb{N}$ is the set of positive rational integers. Let $A = (a_{ij})_{i,j \in \mathbb{N}}$ be a matrix over $\{0,1\}$. For $i \in \mathbb{N}$ we denote by A_{i*} the i-th row of A and by A_{*i} the i-th column of A, i.e.

$$A_{i*} = (a_{i1}, a_{i2}, a_{i3}, \ldots) \text{ and } A_{*i} = \begin{bmatrix} a_{1i} \\ a_{2i} \\ a_{3i} \\ \vdots \end{bmatrix}.$$

We also define the *weight* of a row and a column:

$w(A_{i*}) = |\{j \in \mathbb{N} | a_{ij} = 1\}|$ is the *weight* of the row A_{i*}, and

$w(A_{*i}) = |\{j \in \mathbb{N} | a_{ji} = 1\}|$ is the *weight* of the column A_{*i}.

Let $i \in \mathbb{N}$, and assume $w(A_{i*}) \neq 0$ but finite. Then let

$$k = \min\{j \in \mathbb{N} \mid a_{ij} = 1\} \text{ and } l = \max\{j \in \mathbb{N} \mid a_{ij} = 1\}$$

Now $l-k+1$ is the *length* of the row A_{i*}. Correspondingly we can define the *length* of the column A_{*i}.

Any pair $(i,j) \in \mathbb{N} \times \mathbb{N}$ is called a *cell* of the matrix A. A cell (i,j) is called a

- *flag* if $a_{ij} = 1$ and a
- *galf* if there exists a flag (k,l) such that $a_{kl} = a_{kj} = a_{il} = 1$ and $1 \leq k \neq i$ and $1 \leq l \neq j$.

In the geometric part of the paper, we usually follow the notation in the book of Dembowski [1] or the paper [6].The *union* of two

An *incidence structure* is a triple $(\mathcal{P}, \mathcal{L}, I)$ consisting of two sets $\mathcal{P}$ and $\mathcal{L}$ and a relation $I \subseteq \mathcal{P} \times \mathcal{L}$. For an incidence structure $(\mathcal{P}, \mathcal{L}, I)$ we denote

$$[P] = \{l \in \mathcal{L} \mid P\ I\ l\} \text{ for } P \in \mathcal{P}, \text{ and}$$

$$(l) = \{P \in \mathcal{P} \mid P\ I\ l\} \text{ for } l \in \mathcal{L}.$$

An incidence structure $(\mathcal{P}, \mathcal{L}, I)$ is called a *symmetric tactical configuration* if there exists an integer k such that $|(l)| = |[P]| = k$ for all $l \in \mathcal{L}$ and $P \in \mathcal{P}$ (compare Dembowski [1, pp. 4, 5]). A symmetric tactical configuration is called a *symmetric configuration* (with parameters v_k) if in addition

$$|(l) \cap (l')| \leq 1$$

for $l, l' \in \mathcal{L}$ and $l \neq l'$. The parameters v and k are defined by $|\mathcal{P}| = v$ and $|(l)| = k$ for all $l \in \mathcal{L}$. (Compare Gropp [5]).

Note that the term symmetric configuration is stronger than the term symmetric tactical configuration.

3 The first choice construction

3.1 The matrix A

Let $n \in \mathbb{N}$. We construct a matrix $A(n)$ inductively.

$$A(n) = (a_{ij} \mid i, j \in \mathbb{N})$$

is a $\{0,1\}$-matrix and has the following properties:

(I) There does not exist any pair $((i,j),(k,l))$ of pairs of integers such that

$$a_{ij} = a_{il} = a_{kl} = a_{kj} = 1, \text{ where } i,j,k,l \geq 1,\ i \neq k \text{ and } j \neq l.$$

In other words, A does not contain any rectangles, of which all corners are ones.

(II) Every row of A contains at most $n+1$ ones.

(III) Every column of A contains at most $n+1$ ones.

Note that the Axiom (I) is equivalent to

(I*) There do not exist any 4 integers $i, j, k, l \in \mathbb{N}$ such that $i \neq j,\ k \neq l$ and

$$a_{ik} = a_{il} = a_{jk} = a_{jl} = 1.$$

Or

(I**) A galf is not a flag of A.

We now introduce an inductive construction of $A = (a_{ij}) = A(n)$, the *greedy algorithm*. We start with the 0-matrix. Assume that $k \geq 1$ and that all rows A_{i*} are constructed already for $i < k$. We construct the row A_{k*}. Assume that $l \geq 1$ and that $a_{k1}, a_{k2}, \ldots, a_{k,l-1}$ are constructed already. We denote the matrix that has been constructed by this point as A^{kl} for use later.

Construction of a_{kl}:

- If $\sum_{j<l} a_{kj} \geq n+1$ or $\sum_{i<k} a_{il} \geq n+1$, then $a_{kl} = 0$ remains.
- Otherwise, we check if there exists a pair (i, j) such that

  $$a_{ij} = a_{il} = a_{kj} = 1, \text{ where } 1 \leq i < k \text{ and } 1 \leq j < l.$$

  In this case, again $a_{kl} = 0$ remains.
- If both these conditions are not fulfilled, then we set $a_{kl} = 1$.

The kth row is finished when it contains $n+1$ ones. We shall see below that this is the case after finitely many steps.

Definition 3.1. A row or a column of A^{kl} is called *complete* if its weight is $n+1$.

Lemma 3.2. *Let $k, r \geq 1$ and $\overline{A} = A^{kr}$. The number of galfs for $\overline{A}$ of the form (k, l), $l \geq 1$, is at most xn^2, where x is the number of ones in $\overline{A}_{k*}$.*

Proof. Let (k, l) be a galf for $\overline{A}$. By definition there exists a flag (i, j) such that $i < k,\ j \neq l$ and $a_{ij} = a_{il} = a_{kj} = 1$. Here (k, j) is one of the flags on the row A_{k*}. Starting from (k, j) we have at most n^2 possibilities for l, because there are at most n ones in the column A_{*j} apart from a_{kj}, and at most $n+1$ ones in each row of $\overline{A}$. Hence, altogether, there are at most xn^2 possibilities for l. $\square$

Theorem 3.3. *The length of a row A_{k*}, $k \geq 1$, of A is less than $2n^3 - n(n-3)$.*

Proof. We consider the construction of a row of A. Let $k \geq 1$ and assume that all rows A_{i*} are constructed already for $i < k$. We denote the matrix constructed so far by $\widetilde{A} = A^{k1}$ and construct the kth row A_{k*} according to the above construction of A. For the first one in this row we must put $a_{kl} = 1$, where l is the smallest number such that the lth column of $\widetilde{A}$ contains less than

$n+1$ ones. A cell between the first one and the last one on A_{k*} must be a flag, a galf, or an intersection of A_{k*} with a complete column of $\widetilde{A}$. The number of flags on A_{k*} will be $(n+1)$.

We estimate the number of galfs: By Lemma 3.2, the row A_{k*} contains at most $(n+1)n^2$ galfs (k,i). Here we can do a little better: In the stage before we construct the last one in A_{k*}, say $a_{kr}=1$, we have only n ones in $\overline{A}_{k*}$ ($\overline{A} = A^{kr}$ as above) and hence at most n^3 galfs (k,i) by Lemma 3.1 . Therefore there are at most n^3 galfs of $\overline{A}$ between the first and the last one in the row A_{k*}.

Let $\mathcal{C}$ be the set of complete columns $\widetilde{A}_{*j}$ of $\widetilde{A}$ such that $j>l$. We must find an upper bound for $|\mathcal{C}|$. To do this, we consider the set $\mathcal{L}$ of rows A_{i*} such that $i<k$ and $a_{ij}=1$, for some column $A_{*j}\in\mathcal{C}$. Counting incidences, we find

$$|\mathcal{C}|\cdot\ (n+1)\ \leq\ |\mathcal{L}|\cdot\ n$$

(If $A_{i*}\in\mathcal{L}$, then by the construction of the matrix A, $a_{il}=1$ or $a_{ij}=1$ for some $j<l$. Hence the row A_{l*} contains at most n ones to the right of the column A_{*l}.)

If $A_{i*}\in\mathcal{L}$, $1\leq i<k$, then $a_{il}=1$, or (i,l) is a galf. There are at most n^3 suitable galfs for the column $\overline{A}_{*l}$, by the dual of Lemma 3.1. Hence $|\mathcal{L}|\leq n^3+n$ and $|\mathcal{C}|\leq(n^3+n)n/(n+1)$. This implies that the length of A_{k*} is at most $|\mathcal{C}|+n^3+n+1 = n^3-n^2+2n-2+2/(n+1)+n^3+n+1 = 2n^3-n^2+3n-1+2/(n+1) < 2n^3-n(n-3)$ for $n\geq 2$. Clearly, the theorem is also true for $n=1$ (see Section 5). □

Note that the arguments in the proof of Theorem 3.3 also imply that each row of $A(n)$ contains exactly $n+1$ ones . Also, in the construction of the matrix $A(n)$ described above, the row A_{k*} can be determined after finitely many steps.

3.2 The right edge is monotonously increasing

For each $i\geq 1$ define $g(i)$ to be the smallest j such that $a_{ij}=1$.

Lemma 3.4. *The function g is monotonously increasing*

Proof. Let $i\geq 1$ and remember the construction of the row A_{i*}. Clearly, all the columns A_{*j} must be complete for $1\leq j<g(i)$. Therefore $g(i+1)\geq g(i)$. □

For each $j\geq 1$, define $f(j)$ to be the smallest i such that $a_{ij}=1$.

Lemma 3.5. *The function f is monotonously increasing.*

Proof. Suppose that there are j and k such that $1\leq j<k$ and $f(k)<f(j)$. Remember the construction of the row $A_{f(k)*}$. When $a_{f(k),j}$ is constructed, we have $\sum_{l<j} a_{f(k),l} < n+1$ as $a_{f(k),k}=1$, and $\sum_{l<f(k)} a_{l,j}=0$ because, in the column A_{*j}, we have only zeros above $a_{f(k),j}$. Therefore the first and the second condition in our construction in Section 3.1 are not fulfilled. Hence, we must put $a_{f(k),j}=1$ and $f(j)=f(k)$, a contradiction. □

Remark. Lemma 3.5 also follows from Lemma 3.4 because of the symmetry of A. See Theorem 3.6 below.

3.3 A second, symmetric construction of the matrix A

We introduce an inductive construction of a matrix $C = (c_{ij})$. To start, we set $C = (0)$.

Assume that $k \geq 1$ and that c_{ij} are already constructed for $i, j < k$. We construct the row segment

$$(c_{k,1}, \ldots, c_{k,k})$$

and the column segment

$$\begin{bmatrix} c_{1,k} \\ \vdots \\ c_{k,k} \end{bmatrix}$$

(again, inductively). Assume that $1 \leq l \leq k$, and that $c_{k1}, \ldots, c_{k,l-1}$ and $c_{1k}, \ldots, c_{l-1,k}$ are constructed already. Denote the matrix constructed so far by $C^{kl} = \overline{C}$ and assume that $\overline{C}$ is symmetric and has the properties (I) - (III).

We call the cell (k, l) admissible if:

- There does not exists any pair (i, j) such that $c_{kj} = c_{il} = c_{ij} = 1$, $1 \leq i < k$ and $1 \leq j < l$,
- The number of ones in the row $\overline{C}_{k*}$ is at most n, and
- The number of ones in the column $\overline{C}_{*l}$ is at most n.

Also, the cell (l, k) is called admissible if:

- There does not exists any pair (i, j) such that $c_{ij} = c_{lj} = c_{ik} = 1$, $1 \leq i < l$ and $1 \leq j < k$,
- The number of ones in the row $\overline{C}_{l*}$ is at most n, and
- The number of ones in the column $\overline{C}_{*k}$ is at most n.

Now, because of the symmetry of $\overline{C}$, the cell (k, l) is admissible if and only if (l, k) is admissible. If this is the case, then we put $c_{kl} = c_{lk} = 1$, otherwise $c_{kl} = c_{lk} = 0$. Thus we obtain an extended matrix $C^{k,l+1}$. Clearly, $C^{k,l+1}$ again is symmetric and has the properties (II) and (III). Suppose that $C^{k,l+1}$ contains a forbidden rectangle. Then (k, l) or (l, k), w.l.o.g. (k, l), must be a corner of this rectangle. But this is impossible if (k, l) is admissible. Therefore, the resulting matrix $C^{k,l+1}$ is symmetric and has the properties (I) - (III).

The matrix C actually equals the matrix A which we constructed above. To see this, remember the construction of the coefficients c_{kl} resp. a_{kl} for $1 \leq k, l$. In the row segment $(c_{k,1}, \ldots, c_{k,k-1})$ of C_{k*}, the construction of the coefficients c_{ki} equals the construction of the a_{ki} in the construction of the row A_{k*} anyway (see Section 3.1). Also, $c_{kk} = a_{kk}$.

Consider the column segment

$$\begin{bmatrix} c_{1,k} \\ \vdots \\ c_{k-1,k} \end{bmatrix}$$

and the construction of $c_{lk},\ 1 \le l < k$. Here, a_{lk} arises in the construction of the row A_{l*}. The conditions on the weights of the relevant rows resp. columns are the same in both constructions. There remains the question of the forbidden rectangles. These rectangles are generated by (l,k) and an opposite corner (i,j), where (i,j) lies in a certain area. But this area is the same in both constructions, namely

$$\{(i,j) \mid 1 \le i \le l \text{ and } 1 \le j \le k\}\,.$$

Therefore $c_{lk} = a_{lk}$ and we obtain $a_{ij} = a_{ji}$ for $1 \le i,j$, i.e.

Theorem 3.6. *The matrix A is symmetric.*

Lemma 3.7. *Let $i \ge 1$. There exists j such that $1 \le j \le i$ and $a_{ij} = 1$.*

Proof. Suppose $a_{i1} = \ldots = a_{i,i-1} = 0$. Then by symmetry $a_{1i} = \ldots = a_{i-1,i} = 0$. When constructing the row A_{i*}, we must put $a_{ii} = 1$. □

Remark. (See [8]). Let $k, r \in \mathbb{N}$. There exists exactly one matrix $A = (a_{ij})_{i,j\in\mathbb{N}}$ over $\{0,1\}$ such that $a_{ij} = 1$ if and only if none of the following conditions holds

- There exist $\bar{i} \le i$ and $\bar{j} \le j$ such that $a_{i,\bar{j}} = a_{\bar{i},j} = a_{\bar{i},\bar{j}} = 1$
- $\sum_{\bar{j}<j} a_{i,\bar{j}} \ge k$
- $\sum_{\bar{i}<i} a_{\bar{i},j} \ge r$

This matrix is called the *naive matrix* of Type (k,r).

3.4 The defining matrices

In this section we prove that the matrix A is periodic according to the following definition:

Definition 3.8. If there exist integers $p \ge 1$ and $pp \ge 0$ such that

$$a_{i+p,j+p} = a_{ij} \ for\ all\ i,j > pp,$$

then we call the $\mathbb{N}\times\mathbb{N}-$*matrix A periodic*, p a *period* and pp a *preperiod* of A.

Let $k \ge 2$ and let $\overline{A}$ be the $\mathbb{N}\times\mathbb{N}$-matrix which coincides with A in its first $k-1$ rows, but is 0 otherwise. Let $l(k) = l \ge 1$ be the smallest number, such that the l-th column $\overline{A}_{*l}$ contains fewer than $n+1$ ones. By Lemma 3.5, $\overline{A}_{*l} = 0$ if and only if $\overline{A}$ vanishes on, and to the right of the column $\overline{A}_{*l}$.

Case 1. Assume that $\overline{A}_{*l} = 0$. Clearly, $a_{k1} = \ldots = a_{k,l-1} = 0$ as $\overline{A}_{*i}$ is complete for $1 \le i < l$. By symmetry (Theorem 3.6), also $a_{1k} = \ldots = a_{l-1,k} = 0$. Hence, $k \ge l$ by the minimality of l. On the other hand, by Lemma 3.7, there exists r such that $1 \le r \le l$ and $a_{rl} = 1$. So $\overline{A}_{*l} = 0$ implies $k \le l$, and $k = l$. When we continue the construction of the matrix A and construct a_{kk}, we have exactly the same situation as we had, when we were constructing a_{11}. Therefore we have $a_{i+p,j+p} = a_{ij}$ for $i,j \ge 0$, where $p = k-1$, and A is periodic.

Hence for $pp = 0$ and $p = k - 1$ we have Theorem 3.10 below, except for the last inequality.

In the (more general) case, when $\overline{A}_{*l} \neq 0$, we determine for each $k \geq 2$ a finite $\{0,1\}$-matrix M^k, which determines A_{k*} and all further rows A_{i*} with $i \geq k$. We have an upper bound for the size of M^k. Therefore the matrices M^k will repeat eventually and the matrix A will be periodic after a certain preperiod.

Case 2. Assume that the column $\overline{A}_{*l}$ is not the zero column. Define

$$b = c - l + 1,$$

where c is the largest number such that $a_{rc} = 1$ for some r such that $1 \leq r < k$,

$$d = k - f,$$

where f is the smallest number such that $a_{fl} = 1$, and

$$M^k_{ij} = a_{i+f-1,j+l-1}$$

for $1 \leq i \leq d$ and $1 \leq j \leq b$.

By Lemma 3.5, we know $a_{ij} = 0$ for $i < k$ and $j > c = l + b - 1$, and for $i < f = k - d$ and $j \geq l$. Therefore, the $d \times b$-matrix M^k together with the parameters k and l completely determines the construction of the row A_{k*} and all succeeding rows A_{i*}, $i \geq k$. We call M^k the kth *defining matrix*.

Now $b \leq 2n^3 - n(n-3)$ by Theorem 3.3, and $d \leq 2n^3 - n(n-3) - 1$ because, in addition, the matrix A is symmetric by Theorem 3.6.

(The "height" of a column in A is limited, as is the "length" of a row. Also, by the construction of the row$A_{r,*}$, this row must contain a one on or to the left of the column A_{*l}, as A_{*l} is not complete.)

So the size of the defining matrix M^k is limited. Denote $\sigma = 2n^3 - n(n-3)$ and let us consider all cases from $k = 2$ up to $k = 2^{\sigma^2} + 1$. If for some $k \leq 2^{\sigma^2} + 1$ we have Case 1, then we obtain Theorem with $pp = 0$, $p = k - 1$ and $pp + p = k - 1 \leq 2^{\sigma^2}$. Assume now that Case 1 never occurs. Then two of the resulting matrices M^k must be equal. Let $\overline{p}$ be the smallest number ≥ 1, such that there exists $k \geq 2$ such that

$$M^{k+\overline{p}} = M^k,$$

where $k + \overline{p} \leq 2^{\sigma^2} + 1$, and let $\overline{pp} \geq 1$ be the smallest number such that

$$M^{\overline{pp}+\overline{p}} = M^{\overline{pp}}.$$

The matrix M^k together with the parameters k and $l = l(k)$ determine A_{k*} and the part of the matrix below the row A_{k*}. By the symmetry of A (Theorem 3.6, also by Lemma 3.7 and Theorem 3.3), the ones in A must remain close to the main diagonal. Therefore we have:

Lemma 3.9. *$l(k + \overline{p}) = l(k) + \overline{p}$.*

Hence we have $a_{i+\overline{p},j+\overline{p}} = a_{ij}$ for $i \geq k$. This proves

Theorem 3.10. *There exist integers pp and p such that* $0 \leq pp,\ 1 \leq p$,

$$a_{i+p,j+p} = a_{ij} \ for\ i > pp,\ and$$

$$pp + p \leq 2^{\sigma^2},$$

where $\sigma = 2n^3 - n(n-3)$.

Let p be the smallest number such that there exists $c \geq 0$, such that $a_{i+p,j+p} = a_{ij}$ for $i > c$ and let pp be the smallest number such that $a_{i+p,j+p} = a_{ij}$ for $i > pp$. We call $p = p(n)$ the *period* and $pp = pp(n)$ the *preperiod* for n.

Remark. Clearly the bound for $p(n)$ can easily be improved, e.g. since in view of Lemma 3.5, the upper right hand area of the defining matrix is always 0.

Because of the periodicity, the 'breadth' of the matrix A is limited. That is, the ones of the matrix A remain 'close' to the main diagonal. We define

$$b(n) = \max\left\{|j-i| \mid i,j \geq 1, a_{ij} = 1 \text{ and } i > pp\right\}.$$

Also, the lengths of the rows of A are limited. We define l_{max} to be the *maximum length* of a row A_{i*} with $i > pp(n)$.

Hence, we can always compute the complete Edgar matrix A after finitely many steps.

4 The configuration $\mathcal{E}(n)$

Let $p = p(n)$ and let $pm,\ m \geq 1$, be a multiple of the period such that

$$\left[\frac{pm}{2}\right] > b(n).$$

Denote $\overline{p} = pm$ and $r = \left[\frac{\overline{p}}{2}\right]$. Furthermore, let v be a rational integer larger than or equal to $pp(n) + \overline{p}$. We now define a new matrix $B = (b_{ij})$. B is a $\overline{p} \times \overline{p}$-matrix, and the coefficients of B are defined by

$$b_{ij} = \begin{cases} a_{v+i,v+j} & \text{if } i-r \leq j \leq i+r \\ a_{v+i,v+j-\overline{p}} & \text{if } j > i+r \\ a_{v+i,v+j+\overline{p}} & \text{if } j < i-r \end{cases}$$

for $1 \leq i,j \leq \overline{p}$.

Theorem 4.1. *The weight of every row of B is $n+1$.*

Proof. Let $1 \leq i \leq \overline{p}$. The ith row B_{i*} of B is constructed from the $(v+i)$th row of A, which has weight $n+1$ by the construction of A. Part of B_{i*} is obtained by shifting a segment of the row A_{i*} to the right, respectively to the left. The complementary segment of B_{i*} just remains the same as the corresponding segment of A_{i*}. This together with the inequality $b < \left[\frac{\overline{p}}{2}\right]$ implies that the weights of the rows remain the same. □

Theorem 4.2. *B is symmetric.*

Proof. Let $1 \leq i, j \leq \overline{p}$. If $i - r \leq j \leq i + r$, then $b_{ij} = a_{v+i,v+j} = a_{v+j,v+i}$, because A is symmetric by Theorem 3.6. Also, $i - r \leq j \leq i + r$ implies $j - r \leq i \leq j + r$, so that $a_{v+j,v+i} = b_{ji}$ by definition of B. Finally, if $j < i - r$ (and $i > r$), then

$$b_{ij} = a_{v+i,v+j+\overline{p}} = a_{v+i-\overline{p},v+j} = a_{v+j,v+i-\overline{p}} = b_{ji},$$

where we have the equalities because of the definition of the matrix B by the periodicity of A, the symmetry of A, and, again, the definition of B. □

From Theorem 4.1 and Theorem 4.2 we obtain

Theorem 4.3. *The weight of every column of B is $n + 1$.*

Thus our new (finite!) matrix B again fulfills Axioms (II) and (III). We now prove that B also fulfills Axiom (I).

We use the matrix B as the incidence matrix of an incidence structure. Let $\mathcal{E}(n) = \mathcal{E} = (\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is the set of columns and $\mathcal{L}$ the set of rows of B. Define the incidence

$$B_{*i} \; I \; B_{j*} \Leftrightarrow b_{ji} = 1 \text{ for } 1 \leq i, j \leq \overline{p}$$

$\mathcal{E} = \mathcal{E}(n) = (\mathcal{P}, \mathcal{L})$ is the *Edgar structure* of n. Clearly, $\mathcal{E}(n)$ is a finite symmetric tactical configuration. Also, we have

Theorem 4.4. *$|(a) \cap (b)| \leq 1$ for $a, b \in \mathcal{L}$ and $a \neq b$, if we choose m such that*

$$\overline{p} = pm \geq 2 \cdot l_{max}.$$

Proof. Suppose we have integers i, j, k, l such that $1 \leq i, j, k, l \leq \overline{p} = pm$, $b_{jk} = b_{jl} = b_{il} = b_{ik} = 1$, $i < j$ and $k < l$. We denote the corners of the generated "rectangle" by $C_1 = (j, k)$, $C_2 = (j, l)$, $C_3 = (i, l)$ and $C_4 = (i, k)$. We denote

- $A_1 = \{(i, j) \mid 1 \leq i, j \leq \overline{p} \text{ and } i - r \leq j \leq i + r\}$,
- $B_1 = \{(i, j) \mid 1 \leq i, j \leq \overline{p} \text{ and } j > i + r\}$,
- $B_2 = \{(i, j) \mid 1 \leq i, j \leq \overline{p} \text{ and } j < i - r\}$, and
- $B = B_1 \cup B_1$.

For $1 \leq s \leq 4$ we define c_s by

$$c_s = \begin{cases} 1 & \text{if } C_s \in A_1 \text{ and} \\ 0 & \text{if } C_s \in B = B_1 \cup B_2. \end{cases}$$

So we obtain a vector (c_1, c_2, c_3, c_4). We discuss the 16 possibilities for this vector.

(1111) Here all 4 corners lie in the original matrix A. This is not possible by Axiom I.

(1110) We have

($*$) If a corner C lies in B_1, then any corner above C or to the right of C lies in B_1.

As C_4 lies in B but C_3 not, we find that $C_4 \notin B_1$. On the other hand $C_4 \in B$, but $C_1 \in A$. Hence by the dual of ($*$), $C_4 \notin B_2$, a contradiction. Note that the dual of ($*$) reads

($*d$) If a corner C lies in B_2, then any corner below C or to the left of C lies in B_2.

(1101) By ($*d$), $C_3 = (i, l) \in B_1$. Therefore $l > i + r$ and $b_{il} = a_{v+i,v+l-\overline{p}}$. We have $1 = b_{jk} = a_{v+j,v+k}$ and $1 = b_{jl} = a_{v+j,v+l}$ so that $l - k \leq l_{max} - 1$. Also $1 = b_{il} = a_{v+i,v+l-\overline{p}}$ and $1 = b_{ik} = a_{v+i,v+k}$ so that $k - l + \overline{p} \leq l_{max} - 1$. Hence $\overline{p} \leq 2 \cdot (l_{max} - 2)$.

(1100) By ($*d$), C_3 and C_4 cannot belong to B_2. So $C_3, C_4 \in B_1$. This case is symmetric to the case (0110) below.

(1011) Here $C_2 \in B$. If $C_2 \in B_1$, then $C_3 \in B_1$ by ($*$). So $C_2 \in B_2$, and $C_1 \in B_2$ by ($*d$), a contradiction.

(1010) leads to a contradiction as (1011).

(1001) Here $C_2, C_3 \in B_1$ by ($*d$). We have $b_{ik} = a_{v+i,v+k} = b_{jk} = a_{v+j,v+k} = 1$ and $b_{il} = a_{v+i,v+l-\overline{p}} = b_{jl} = a_{v+j,v+l-\overline{p}} = 1$. This contradicts Axiom I. (Note that $l \leq \overline{p}$ so that $v + l - \overline{p} < v + k$.)

(1000) $C_2 \in B$ and $C_1 \in A_1$ implies $C_2 \in B_1$ by ($*d$). We have

($**$) If a corner C belongs to $B_i, i \in \{1, 2\}$, then any corner which lies in $B = B_1 \cup B_2$ and directly below, above, to the right or to the left of C again lies in B_i. (Note that no row of B contains a cell of B_1 and a cell of B_2 at the same time: Suppose we have $(i, j) \in B_1$ and $(i, j') \in B_2$. Then $j > i + r$ and $i < j - r \leq \overline{p} - r \leq r + 1$. On the other hand, $j' < i - r$ and $i > j' + r \geq 1 + r$, a contradiction.)
By this Lemma $C_3, C_4 \in B_1$. Therefore $l > j + r$ and $k, l > i + r$. Analogous to the case (1101) we have $1 = b_{ik} = a_{v+i,v+k-\overline{p}}$ and $1 = b_{il} = a_{v+i,v+l-\overline{p}}$ so that $l - k \leq l_{max} - 1$. Also $1 = b_{jl} = a_{v+j,v+l-\overline{p}}$ and $1 = b_{jk} = a_{v+j,v+k}$ so that $k - l + \overline{p} \leq l_{max} - 1$. As in Case (1101) we obtain $\overline{p} \leq 2 \cdot (l_{max} - 2)$, contradicting our assumption.

(0111) $C_1 \in B_2$ by ($*$). This is symmetric to the case (1101).

(0110) $C_1 \in B$ and $C_2 \in A_1$ implies $C_1 \in B_2$ by ($*$). In the same way we see that $C_4 \in B_2$. As in case (1001) we can prove that this is impossible.

(0101) $C_1 \in B$ and $C_2 \in A_1$ implies $C_1 \in B_2$. $C_3 \in B$ and $C_4 \in A_1$ implies $C_3 \in B_1$.
We construct from our 'rectangle' in the matrix B a 'rectangle' in the matrix A. We have
$a_{v+i,v+l-\overline{p}} = b_{il} = 1,$
$a_{v+i,v+k} = b_{ik} = 1,$
$a_{v+j-\overline{p},v+k} = a_{v+j,v+k+\overline{p}} = b_{jk} = 1$, and
$a_{v+j-\overline{p},v+l-\overline{p}} = a_{v+j,v+l} = b_{jl} = 1,$
because $C_3 = (i,l) \in B_1,\ C_4 = (i,k) \in A_1,\ C_1 = (j,k) \in B_2,\ C_2 = (j,l) \in A_1$, and because A is periodic with period p. But this contradicts Axiom (I). (Note that $v+j-\overline{p} \neq v+i$ and $v+l-\overline{p} \neq v+k$ because $j-i, k-l < \overline{p}$.) Hence this case is not possible.

(0100) $C_1 \in B$ and $C_2 \in A$ implies $C_1 \in B_2$ by $(*)$. By $(**)$ we obtain $C_4 \in B_2$ and $C_3 \in B_2$. Thus $C_2 \in B_2$ by $(*d)$, a contradiction.

(0011) $C_4 \in A$ and $C_1 \in B$ implies $C_1 \in B_2$ by $(*)$. Also $C_2 \in B_2$. This case is symmetric to (1001) and hence impossible.

(0010) $C_2 \in B$ and $C_3 \in A_1$ implies $C_2 \in B_2$ by $(*)$. Hence $C_1, C_4 \in B_2$ by $(**)$. Symmetric to (1000).

(0001) $C_4 \in A_1$ and $C_1 \in B$ implies $C_1 \in B_2$ by $(*)$. Hence $C_2, C_3 \in B_2$ by $(**)$. But $C_3 \in B_2$ and $C_4 \in A_1$ is impossible by $(*d)$.

(0000) By $(**)$, $C_1, C_2, C_3, C_4 \in B_1$ or $C_1, C_2, C_3, C_4 \in B_2$. Impossible by Axiom (I). □

Hence, $\mathcal{E}(n)$ is a symmetric configuration with parameters $\overline{p}_{n+1}$ (i.e. with a point set of cardinality $\overline{p}$ and $n+1$ points on every line). Note that we obtain a symmetric configuration for every m which is sufficiently large. Thus we actually have a series of configurations.

As a consequence of Theorem 4.4 we obtain

Corollary 4.5. *For every integer $k \geq 1$ there exists a finite symmetric configuration with k points on each line.*

5 Examples

We know the structure of $\mathcal{E}(n)$ for infinitely many n. In spite of this, actually computing the symmetric configuration $\mathcal{E}(n)$ is, in general, not so simple. For relatively small n the computations already become extremely unwieldy. Take $n = 3$. In this case, the preperiod is 48, and the period is 16. $\mathcal{E}(3)$ is a symmetric configuration with parameters 16_4 as defined in Gropp [5]. (See Fig. 1, for the Martinetti graph (see Gropp[5]), Fig. 2). Its automorphism group has order 2.

For $n = 1,\ 2,\ 4$, and 16, we find that the preperiod is 0 and the period is $p = n^2 + n + 1$. For these orders (where the Case 1 in Section 3.4 actually occurs) we can use a more compact construction replacing $\mathcal{E}(n)$. We just take

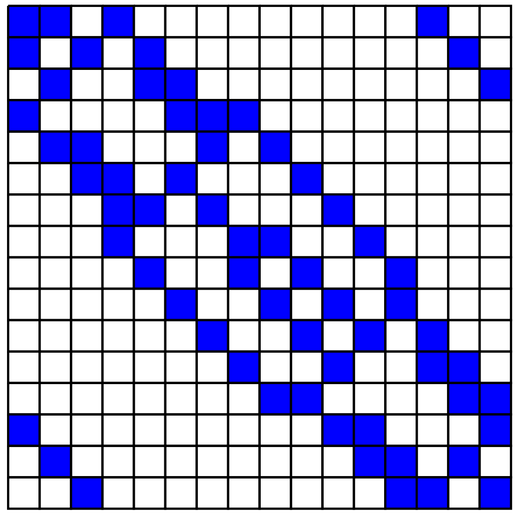

Figure 1: Incidence matrix of $\mathcal{E}\,(3)$

$\overline{B} = (\bar{b}_{ij})$ to be the $p \times p$-matrix with coefficients $\bar{b}_{ij} = a_{ij}$ for $1 \leq i, j \leq p$. Taking $\overline{B}$ as incidence matrix we construct an incidence geometry $\overline{\mathcal{E}} = \overline{\mathcal{E}}(n)$ as above. Actually, for $n \geq 2$ the incidence structure $\overline{\mathcal{E}}(n)$ in these cases is just a projective plane of order n which turns out to be desarguesian. For $n = 1$, we obtain just a triangle, hence a degenerate projective plane. Here

$$\overline{B} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

The original Edgar structure $\mathcal{E}\,(n)$ for $m = 2$ and a suitable v in these cases is just the 'union', in some sense, of two copies of $\overline{\mathcal{E}}(n)$.

Note hat thereby we have a completely geometric simple construction of, e.g., the Galois field GF(16).

In a forthcoming paper [8] we shall prove that, for every Fermat 2-power, that is, a number of the format $n = 2^{2^a}$ for $a \geq 0$, $\overline{\mathcal{E}}(n) \cong \mathrm{PG}(2,\, n)$.

Apparently the system favors Fermat 2 powers. Until now we could not discover, why this is the case.

As a further example, calculating $n = 5$ takes quite a deal of patience. Hans-Joerg Schaeffer calculated that the preperiod is at least 5,652,533. However, $\mathcal{E}\,(5)$ holds a surprise, as we find that the period is just 31, and $\mathcal{E}\,(5)$ is isomorphic to the projective plane of order 5.

Now of course it would be very interesting to calculate $\mathcal{E}\,(6)$ and $\mathcal{E}\,(10)$ for example, because it is known that projective planes of these orders do not exist (by Euler [3], Lam [9], and MacWilliams, Sloane and Thompson [11]). Unfortunately, we did, until today, not succeed in determining $\mathcal{E}\,(10)$. For $n = 6$,

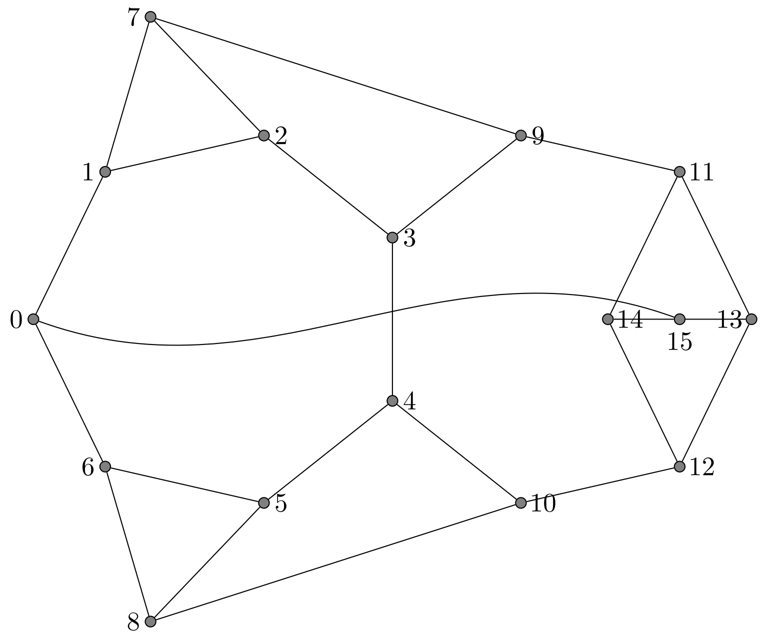

Figure 2: Martinetti graph of $\mathcal{E}\,(3)$

we could find an upper bound for the preperiod of 15 trillion lines, while the period is $1,411,455,772,046 = 1,335,167 * 9,973 * 53 * 2$.

Since we cannot store even a sparse matrix with 15 trillion lines and 7 points in each line, we store only a small amount of lines (about 1 million), which enables us to compute the next line, while forgetting the oldest lines. This allows us to search for cycles up to a length of about one million, which is sufficient up to order 5. For order 6, we use the cycle finding algorithm of Floyd [4]. The key idea of this algorithm is to compute for every k, the rows in the intervals $[k, k + n^2 + n + 1]$ and $[2k, 2k + 2(n^2 + n + 1)]$ and check if the rows in the first interval appear in the second interval.

It would be extremely interesting if $\mathcal{E}\,(10)$ could somehow be calculated.

Many more interesting cases, some of which emerge after a rather short computation, can be found if we extend our investigations to non-symmetric configurations (see [8]).

Remark. Every $\{0, 1\}$-matrix determines its *galf-matrix* $\mathcal{G}(X)$. This matrix can be computed using the program set ProjFinder [10], and so we obtain an easy way to determine the matrix $A(n)$.

References

[1] **Dembowski, P.:** Finite Geometries. Ergebnisse der Mathematik und ihrer Grenzgebiete **44**, Springer-Verlag, Heidelberg (1968).

[2] **Edgar, T.:** First-best Projective Planes and Related Structures. Diplomarbeit, Tuebingen (2009)

[3] **Euler, L.:** Recherches sur une nouvelle espèce des quarrés magiques. Verh. Zeeuwsch. Genootsch. Wetensch. Vlissingen **9** (1782) 85-239.

[4] **Floyd, R.W.:** Non-deterministic Algorithms. J. ACM **14** (1967) 636-644.

[5] **Gropp, H.:** Configurations and Their Realization. Discr. Math. **174** (1997) 137-151.

[6] **Hering, C.H. and A. Krebs:** A partial plane of order 6 constructed from the icosahedron. Des. Codes Cryptogr. **44** (2007) 287-292.

[7] **Krebs, A.:** Projektive Ebenen und Inzidenzmatrizen. Diplomarbeit, Tübingen (2006).

[8] **Krebs, A., C.H. Hering, and T. Edgar:** First choice constructions for non-symmetric configurations. to appear.

[9] **Lam, C.W.H.:** The search for a finite projective plane of order 10. Amer. Math. Monthly **98** (1991) 305-318.

[10] **ProjFinder:**

http://www.mathematik.uni-tuebingen.de/ab/gruppen/hering/main.html

[11] **MacWilliams, F.C., N.J.A. Sloane and J.G. Thompson:** On the existence of a projective plane of order 10. J. Comb. Theory **14 A** (1973) 66-78.